

Pengamanan File Citra Digital Dengan Menggunakan Metode Least Significant Bit Dan End Of File

¹Hertika Yuni Asti Sinaga, ²Lamhot Sitorus

¹Teknik Informatika Unika St. Thomas S.U; Jln. Setia Budi No.479-F Medan, 061-8210161

²Teknik Informatika Unika St. Thomas S.U; Jln. Setia Budi No.479-F Medan, 061-8210161

e-mail : hertikasinaga@gmail.com; ²lamhot68@yahoo.com

Abstrak

Steganografi keamanan data (gambar) merupakan hal yang sangat penting didalam dunia modern saat ini. Hal ini semakin diperkuat dengan kebutuhan bisnis untuk menjaga kerahasiaan data yang sangat penting untuk dirahasiakan. Banyak terjadi manipulasi gambar dengan bentuk yang negatif dan membuat pemilik gambar asli merasa dirugikan karena gambar telah dimanipulasi dan menunjukkan citra yang buruk. Data yang bersifat rahasia dibuatkan sistem penyimpanan dan pengirimannya agar tidak terbaca atau diubah oleh orang-orang yang tidak bertanggung jawab, baik saat data tersebut tersimpan sebagai file gambar didalam komputer maupun saat data tersebut dikirim melalui internet seperti email, dan media penyimpanan online lainnya. Oleh karena itu digunakan algoritma Least Significant Bit dan End Of File untuk meningkatkan keamanan sebuah gambar. Sistem yang akan dibangun dalam penelitian ini akan menciptakan sebuah aplikasi yang dapat menyisipkan gambar kedalam gambar. Gambar yang bersifat rahasia akan disisipkan kedalam gambar sehingga gambar tersebut tetap aman dari orang-orang yang bermaksud memanipulasi gambar tersebut.

Kata kunci : Steganografi, Least Significant Bit, End Of File

Abstract

Data security steganography (image) is very important in the modern world today. This is further strengthened by the business needs to maintain the confidentiality of data that is very important to be kept secret. A lot of image manipulation takes place with a negative shape and makes the original image owner feel aggrieved because the image has been manipulated and shows a bad image. Confidential data is created for storage and delivery systems to be unreadable or modified by irresponsible people, either when the data is stored as an image file within the computer or when data is sent over the internet such as email, and other online storage media. Therefore we use Least Significant Bit and End Of File algorithm to improve the security of an image. The system to be built in this research will create an application that can insert images into the picture. Confidential images will be inserted into the image so that the image remains secure from those who intend to manipulate the image.

Keywords : Steganography, Least Significant Bit, End Of File

1. PENDAHULUAN

Meningkatnya penggunaan teknologi informasi, yang menggunakan komputer sebagai medianya maka keamanan data adalah aspek yang sangat penting dalam sistem teknologi informasi. Terutama dalam menghadapi persaingan bisnis. Salah satu citra digital adalah dokumen gambar yang sering tidak diperdulikan dampak negatifnya bila dimanfaatkan orang yang tidak berhak. Banyak terjadi manipulasi gambar dengan bentuk yang negatif dan membuat pemilik gambar yang asli merasa dirugikan karena gambar yang telah dimanipulasi telah menunjukkan citra yang buruk.

Data yang bersifat rahasia perlu dibuatkan sistem penyimpanan dan pengirimannya agar tidak terbaca atau diubah oleh orang-orang yang tidak bertanggung jawab, baik saat data tersebut tersimpan sebagai file gambar didalam komputer maupun saat data tersebut dikirim melalui internet seperti email, dan media penyimpanan online lainnya. File citra digital atau gambar terkadang merupakan sesuatu aset yang berharga. Misalkan saja seorang pegawai pada divisi engineering yang bekerja disebuah perusahaan yang bergerak dibidang produksi mobil akan mengirim design gambar kendaraan khusus berupa hard copy kepada divisi kendaraan khusus melalui internet. Design gambar kendaraan tersebut perlu diamankan agar tidak diketahui atau ditiru oleh competitor (pesaing) perusahaan tersebut. Untuk mengamankan gambar yang di kirimkan melalui media internet, maka diperlukan suatu teknik keamanan yaitu Steganografi.

Steganografi adalah teknik yang digunakan untuk menyembunyikan informasi ke dalam sebuah media, bisa berupa media gambar, suara ataupun video. Pada steganografi media gambar dikenal sebuah teknik yang dinamakan *Least Significant Bit* (LSB). Metode penyisipan LSB (*Least Significant Bit*) ini adalah menyisipi pesan dengan cara mengganti bit ke 8, 16 dan 24 pada representasi biner file gambar dengan representasi biner pesan rahasia yang akan disembunyikan.

Teknik EOF atau End Of File merupakan salah satu teknik yang digunakan dalam steganografi. Teknik ini menggunakan cara dengan menyisipkan data pada file. Teknik ini dapat digunakan untuk menyisipkan data yang ukurannya sesuai dengan kebutuhan. Ukuran file yang telah disisipkan data sama dengan ukuran file sebelum disisipkan data ditambah dengan ukuran data yang disisipkan data ditambah dengan ukuran data yang disisipkan kedalam file tersebut.

2. METODOLOGI PENELITIAN

II.1 Sejarah Steganografi

Menurut (Munir, 2004) Steganografi sudah dikenal oleh bangsa Yunani. Herodatus, penguasa Yunani, mengirim pesan rahasia dengan menggunakan kepala budak atau prajurit sebagai media. Dalam hal ini, rambut budak dibotaki, lalu pesan rahasia ditulis pada kulit kepala budak. Ketika rambut budak tumbuh, budak tersebut diutus untuk membawa pesan rahasia di balik rambutnya. Bangsa Romawi mengenal steganografi dengan menggunakan tinta tak-tampak (*invisible ink*) untuk menuliskan pesan. Tinta tersebut dibuat dari campuran sari buah, susu, dan cuka. Jika tinta digunakan untuk menulis maka tulisannya tidak tampak. Tulisan di atas kertas dapat dibaca dengan cara memanaskan kertas tersebut. Sebagai contoh ilustrasi, di bawah ini adalah citra lada (peppers.bmp) yang akan digunakan untuk menyembunyikan sebuah dokumen word (hendro.doc). Steganografi (*steganography*) adalah ilmu dan seni menyembunyikan pesan rahasia (*hiding message*) sedemikian sehingga keberadaan (eksistensi) pesan tidak terdeteksi oleh indera manusia. Kata steganografi berasal dari Bahasa Yunani yang berarti “tulisan tersembunyi” (*covered writing*). Steganografi membutuhkan dua properti: wadah penampung dan data rahasia yang akan disembunyikan. Steganografi digital menggunakan media digital sebagai wadah penampung, misalnya citra, suara, teks, dan video. Data rahasia yang disembunyikan juga dapat berupa citra, suara, teks, atau video. Steganografi dapat dipandang sebagai kelanjutan kriptografi. Jika pada kriptografi, data yang telah disandikan (*ciphertext*)

tetap tersedia, maka dengan steganografi cipherteks dapat disembunyikan sehingga pihak ketiga tidak mengetahui keberadaannya. Di negara-negara yang melakukan penyensoran informasi, steganografi sering digunakan untuk menyembunyikan pesan-pesan melalui gambar (*images*), video, atau suara (*audio*).

2.2 Defenisi Steganografi

Menurut (Sadikin, 2012) Steganografi adalah ilmu menyembunyikan teks pada media lain yang telah ada sedemikian sehingga teks yang tersembunyi menyatu dengan media itu. Media tempat penyembunyian pesan tersembunyi dapat berupa media teks, gambar, audio atau video. Steganografi yang kuat memiliki sifat media yang telah tertanam teks tersembunyi sulit dibedakan dengan media asli namun teks tersembunyi tetap dapat diekstrasi. Contoh sederhana teknik steganografi pada media gambar misalnya dengan mengubah nilai LSB (*least significant bit*) pada byte intensitas piksel dengan teks yang ingin disembunyikan. Misalnya pada gambar *gray level* piksel direpresentasikan sebagai 1 byte. Jika terdapat 8 piksel bernilai {*FF, A0, CD, 18, 92, 34, E2, B1*} (dalam heksa desimal) dan huruf pada teks yang ingin disembunyikan adalah "S" dengan nilai ASCII "S" adalah 53 (dalam heksimal) atau (01010011). Proses steganografi dengan LSB menghasilkan gambar dengan pesan yang tersembunyi dengan deretan piksel bernilai {*FE, A1, CC, 19, 92, 34, E3, B1*}. mengilustrasikan proses penyisipan ini. Untuk mendapatkan teks tersembunyi kembali cukup dengan membaca LSB Tiap piksel.

2.3 Kriteria Steganografi

Menurut (Munir, 2004) Penyembunyian data rahasia ke dalam citra digital akan mengubah kualitas citra tersebut. Kriteria yang harus diperhatikan dalam penyembunyian data adalah:

1. *Fidelity*
Mutu citra penampung tidak jauh berubah. Setelah penambahan data rahasia, citra hasil steganografi masih terlihat dengan baik. Pengamat tidak mengetahui kalau di dalam citra tersebut terdapat data rahasia.
2. *Robustness*
Data yang disembunyikan harus tahan terhadap manipulasi yang dilakukan pada citra penampung (seperti perubahan kontras, penajaman, pemampatan, rotasi, perbesaran gambar, pemotongan (*cropping*), enkripsi, dan sebagainya). Bila pada citra dilakukan operasi pengolahan citra, maka data yang disembunyikan tidak rusak.
3. *Recovery*
Data yang disembunyikan harus dapat diungkapkan kembali (*recovery*). Karena tujuan steganografi adalah *data hiding*, maka sewaktu-waktu data rahasia di dalam citra penampung harus dapat diambil kembali untuk digunakan lebih lanjut.

2.4 Teknik Steganografi

Menurut (Armada, 2012) Pada dasarnya, terdapat tujuh teknik yang digunakan dalam steganography :

1. *Injection*
Merupakan suatu teknik menanamkan pesan rahasia secara langsung ke suatu media. Salah satu masalah dari teknik ini adalah ukuran media yang diinjeksi menjadi lebih besar dari ukuran normalnya sehingga mudah dideteksi. Teknik itu sering juga disebut Embedding.
2. *Substitusi*
Data normal digantikan dengan data rahasia. Biasanya, hasil teknik itu tidak terlalu mengubah ukuran data asli, tetapi tergantung pada file media dan data yang akan disembunyikan. Teknik substitusikan bisa menurunkan kualitas media media yang ditumpangi.

3. Transporm Dominan
Teknik ini sangat efektif. Pada dasarnya, transpormasi domain menyembunyikan pada data “ transporm space”. Akan sangat lebih efektif bila teknik ini diterapkan pada file berekstensi Jpeg (gambar).
4. Spread Spectrum
Sebuah teknik pentransmisian menggunakan *pseudo-noise code*, yang independen terhadap data informasi sebagai modulator bentuk gelombang untuk menyebarkan energy sinyal dalam sebuah jalur gelombang untuk menyebarkan energi sinyal dalam sebuah jalur komunikasi (*bandwidth*) yang lebih besar dari pada sinyal jalur komunikasi informasi. Oleh penerima, sinyal dikumpulkan kembali menggunakan replika *pseudo-noise code* tersinkronisasi.
5. Statisikal Method
Teknik ini disebut juga skema steganographic 1 bit. Skema tersebut menanamkan satu bit informasi pada media tumpangan dan mengubah statistik walaupun hanya 1 bit Perubahan statistik ditunjukkan dengan indikasi 1 dan jika tidak ada perubahan, terlihat indikasi 0. Sistem ini bekerja berdasarkan kemampuan penerima dalam membedakan antara informasi yang dimodifikasi dan yang belum.
6. Distortion
Metode ini menciptakan perubahan atas benda yang ditumpangi oleh data rahasia.
7. Cover Generation
Metode ini lebih unik dari pada metode lainnya karena cover object yang dipilih untuk menyembunyikan pesan. Contoh dari metode ini adalah spam mimic.

2.5 Citra Digital

Menurut (Pehtian, 2014) Citra digital merupakan suatu array dua dimensi atau suatu matriks yang elemen-elemennya menyatakan tingkat keabuan dari elemen gambar. Jadi informasi yang terkandung bersifat diskrit. Citra digital merupakan representatif dari citra yang diambil oleh mesin dengan bentuk pendekatan berdasarkan sampling dan kuantisasi. Sampling menyatakan besarnya kotak-kotak yang disusun dalam baris dan kolom atau dengan kata lain sampling pada citra menyatakan besarnya nilai tingkat kecerahan yang dinyatakan dalam nilai tingkat keabuan (grayscale) sesuai dengan jumlah bit biner yang digunakan oleh mesin atau dengan kata lain kuantisasi pada citra menyatakan jumlah warna yang ada pada citra. Berdasarkan jumlah tingkat kuantisasi dan warnanya, sebuah citra digital juga bisa dikelompokkan menjadi dua jenis :

1. Gambar Bitmap
Gambar bitmap sering disebut juga dengan gambar raster. Gambar bitmap adalah gambar yang terbentuk dari pixel, dengan sikap pixelnya mempunyai warna tertentu. Jika gambar bitmap ini diperbesar, misalnya 4 kalinya, maka gambar akan menjadi kabur karena pixelnya juga bertambah besar menjadi 4 kalinya (kualitas gambar menurun).
Format gambar bitmap sering dipakai dalam foto dan gambar. Dua istilah yang perlu dipahami ketika bekerja dengan gambar bitmap adalah resolusi dan kedalaman warna. Gambar bitmap biasanya diperoleh dari proses : scanner, camera digital, video capture. Contoh filenya bmf,gif,jpg.
2. Gambar vektor
Gambar dihasilkan dari perhitungan matematis dan tidak berdasarkan pixel. Jika gambar diperbesar atau diperkecil, kualitas gambar relatif tetap baik dan tidak berubah. Gambar vektor biasanya dibuat menggunakan aplikasi-aplikasi gambar vektor misalkan: Corel Draw, Adobe Illustrator, Macromedia Freehand. Contoh filenya pdf.

2.6 Metode Least Significant Bit

Menurut (Andrian, 2012) Pendekatan paling sederhana untuk menyembunyikan data dalam file citra disebut penyisipan *Least Significant Bit* (LSB). Penyisipan *Least significant bit*

(LSB) adalah pendekatan yang umum untuk menanamkan informasi dalam media citra. *Least significant bit* (dengan kata lain, bit ke-8) sebagian atau seluruh dari *byte* dalam sebuah gambar diubah menjadi sebuah *bit* dari pesan rahasia. Bila menggunakan gambar 24-bit, *bit* dari masing-masing komponen warna merah, hijau dan biru dapat digunakan, karena masing-masing ditampilkan dalam bentuk *byte*. Dengan kata lain, seseorang dapat menyimpan 3 bit di setiap pixel. Citra dengan piksel 800×600 , dapat menyimpan total Jumlah 1,440,000 *bit* atau 180.000 *byte* data yang disisipkan. Dalam metode yang ada, dibutuhkan representasi biner dari data yang akan disembunyikan dengan metode LSB. Sebagai contoh, misalkan kita memiliki tiga piksel yang berdekatan (sembilan *bytes*) dengan kode RGB berikut :

```
00110101 11010110 11101010
11110100 00111001 11100001
01110001 10010001 11100001
```

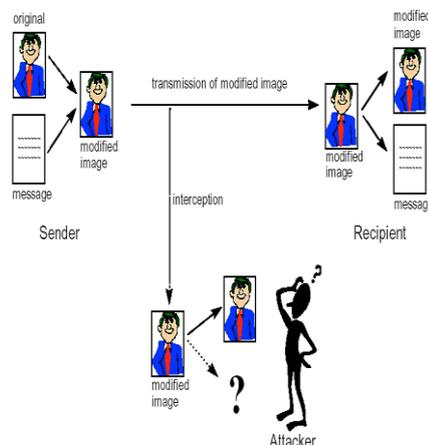
Pesan yang akan disisipkan adalah karakter “R”, yang nilai binernya adalah “01010010”, maka akan dihasilkan citra hasil dengan urutan bit sebagai berikut:

```
00110100 11010111 11101010
11110101 00111000 11100000
01110001 10010000 11100001
```

Pada contoh di atas, dapat dilihat bahwa sebagian *bit* LSB yang ada pada citra asal (original) digantikan dengan bit dari pesan yang akan disisipkan. Satu karakter = 1 *byte* = 8 *bit* pesan akan memerlukan 8 lokasi tempat penyisipan *bit* pesan. Jika menggunakan citra *grayscale* berarti memerlukan 8 piksel dari citra yang akan disisipi pesan. Jika menggunakan citra berwarna (RGB) berarti memerlukan 3 piksel dari citra yang akan disisipi pesan. Pada saat penyisipan pesan, ada piksel yang berubah dari piksel asal, ada juga piksel yang tidak berubah sama sekali. Hal ini dikarenakan *bit* pesan yang akan disisipkan nilainya sama dengan *bit* LSB dari piksel citra yang akan disisipi pesan.

2.7 Konsep Steganografi

Menurut (Wijaya,dkk, 2015) mengatakan bahwa Steganografi adalah ilmu pengetahuan dan seni dalam menyembunyikan komunikasi. Suatu sistem Steganografi sedemikian rupa menyembunyikan isi suatu data di dalam suatu sampul media yang tidak dapat di duga oleh orang biasa sehingga tidak membangunkan suatu kecurigaan kepada orang yang melihatnya, dapat di lihat dalam Gambar 2.1. Di masa lalu, orang-orang menggunakan tato tersembunyi atau tinta tak terlihat untuk menyampaikan isi *Steganografi*. Hari ini, teknologi jaringan dan komputer menyediakan cara yang mudah dalam menggunakan jaringan komunikasi untuk *Steganografi*.

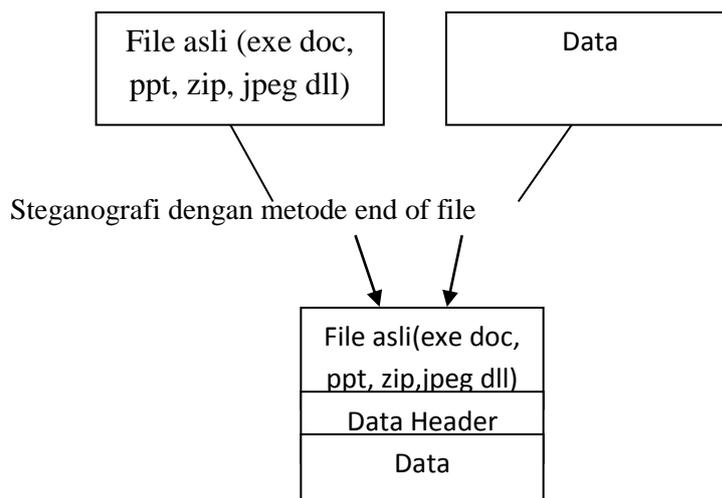


Gambar 2.1 Proses umum tentang proses Steganografi
(Sumber : Zollner, 2015)

Provos & Honeyman berpendapat tujuan *Steganografi* modern adalah untuk mempertahankan suatu media yang tidak bisa mendeteksi, tetapi karena sistem *Steganografi* masih memiliki kelemahan yang meninggalkan jejak dibelakang sampul media sehingga dapat ditemukan. Sekalipun isi rahasiatidaklah diungkapkan, keberadaan tentang memodifikasisampul media dapat merubah sifat statistik, jadi para penelitidapat mendeteksi distorsi dihasil dari proses media stegodengan sifat statistik. Maka proses untuk pencarian danmendeteksi penyimpanan di dalam media yang distorsidisebut sebagai “*Statistical Steganalysis*”.

2.8 Metode End Of File (EOF)

Menurut (Martono, Irawan, 2013) Secara umum teknik steganografi menggunakan *redundant bits* sebagai tempat menyembunyikan pesan pada saat dilakukan kompresi data, dan kemudian menggunakan kelemahan indera manusia yang tidak sensitive sehingga pesan tersebut tidak ada perbedaan yang terlihat. Teknik EOF atau *End Of File* merupakan salah satu teknik yang digunakan dalam steganografi. Teknik ini digunakan dengan cara menambahkan data atau pesan rahasia pada akhir file. Perhitungan ukuran file yang telah disisipkan data sama dengan ukuran file sebelum disisipkan data ditambah ukuran data rahasia yang telah diubah menjadi *encoding file*. Dengan metode EOF, secara umum media steganografi (file yang akan disisipi data) memiliki struktur seperti gambar dibawah ini:



Gambar 2.2 Struktur File Steganografi dengan Metode EoF
(Sumber : Martono ,2013)

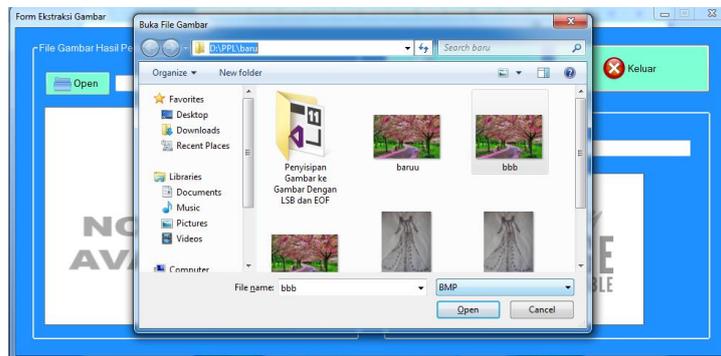
Penanda data header atau flag akan kita letakkan di awal atau akhir file, di mana tidak ada looping yang digunakan untuk mencarinya. Pada beberapa file seperti exe dan zip, penempatan flag di awal file asli tidak akan menjadi masalah,namun untuk jenis file lain semisal JPG, BMP dan DOC, penempatan flag di awal file akan merusak file asli karena mengganggu isi file asli dan merusak CRC file tersebut.

3. HASIL DAN PEMBAHASAN

3.1. Hasil Sistem

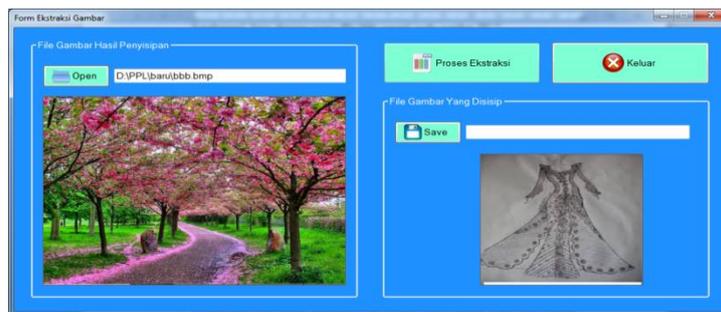
Setelah tahap implementasi selesai, maka akan dilanjutkan pada tahap berikutnya yaitu tahap pengujian sistem. Dalam hal ini akan di uji coba dalam melakukan proses penyisipan gambar sehingga dapat diketahui keberhasilan dari sistem yang dibangun.

Sebelum melakukan ekstraksi gambar user harus memilih tombol open untuk melakukan ekstraksi gambar, gambar yang akan diekstrak yaitu gambar yang berekstensi .



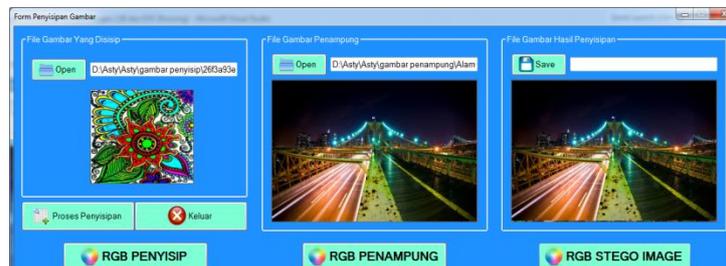
Gambar 3.1 Proses Pengambilan Gambar

Setelah itu tekan tombol open maka gambar yang akan diekstrak muncul di file gambar hasil penyisipan, kemudian klik tombol proses ekstraksi maka akan muncul gambar awal sebelum dilakukan proses penyisipan.



Gambar 3.2 Proses Ekstraksi Gambar

3.2. Pembahasan



Gambar 3.3 Contoh Gambar Pengujian Sistem

Tabel 4.1 Nilai RGB Pada Gambar Diatas

Nilai RGB Penyisip	Nilai RGB Penampung	Nilai RGB Stego Image
(0,0) R = 255 = 11111111 G = 255 = 11111111 B = 255 = 11111111	(0,0) R = 104 = 01101000 G = 104 = 01101000 B = 104 = 01101000	(0,0) R = 105 = 01101001 G = 105 = 01101001 B = 105 = 01101001
(0,1) R = 55 = 00110111 G = 59 = 00111011 B = 59 = 00111011	(1,0) R = 100 = 01100100 G = 100 = 01100100 B = 100 = 01100100	(1,0) R = 101 = 01100101 G = 101 = 01100101 B = 101 = 01100101
(0,2) R = 16 = 00010000 G = 41 = 00101001 B = 20 = 00010100	(2,0) R = 101 = 01100101 G = 101 = 01100101 B = 101 = 01100101	(2,0) R = 101 = 01100101 G = 101 = 01100101 B = 101 = 01100101
(0,3) R = 67 = 01000011 G = 240 = 11110000 B = 155 = 10011011	(3,0) R = 100 = 01100100 G = 100 = 01100100 B = 100 = 01100100	(3,0) R = 101 = 01100101 G = 101 = 01100101 B = 101 = 01100101
(0,4) R = 0 = 00000000 G = 31 = 00011111 B = 5 = 00000101	(4,0) R = 100 = 01100100 G = 100 = 01100100 B = 100 = 01100100	(4,0) R = 101 = 01100101 G = 101 = 01100101 B = 101 = 01100101
(0,5) R = 0 = 00000000 G = 0 = 00000000 B = 0 = 00000000	(5,0) R = 100 = 01100100 G = 100 = 01100100 B = 100 = 01100100	(5,0) R = 101 = 01100101 G = 101 = 01100101 B = 101 = 01100101
(0,6) R = 0 = 00000000 G = 0 = 00000000 B = 0 = 00000000	(6,0) R = 100 = 01100100 G = 100 = 01100100 B = 100 = 01100100	(6,0) R = 101 = 01100101 G = 101 = 01100101 B = 101 = 01100101
(0,7) R = 0 = 00000000 G = 0 = 00000000 B = 0 = 00000000	(7,0) R = 100 = 01100100 G = 100 = 01100100 B = 100 = 01100100	(7,0) R = 101 = 01100101 G = 101 = 01100101 B = 101 = 01100101
(0,8) R = 0 = 00000000 G = 0 = 00000000 B = 0 = 00000000	(8,0) R = 100 = 01100100 G = 100 = 01100100 B = 100 = 01100100	(8,0) R = 101 = 01100101 G = 101 = 01100101 B = 100 = 01100100
(0,9) R = 8 = 00001000 G = 55 = 00110111 B = 35 = 00100011	(9,0) R = 100 = 01100100 G = 100 = 01100100 B = 100 = 01100100	(9,0) R = 100 = 01100100 G = 100 = 01100100 B = 101 = 01100101

(0,10) R = 38 = 00100110 G = 108 = 01101100 B = 87 = 01010111	(10,0) R = 100 = 01100100 G = 100 = 01100100 B = 100 = 01100100	(10,0) R = 101 = 01100101 G = 100 = 01100100 B = 101 = 01100101
(0,11) R = 7 = 00000111 G = 0 = 00000000 B = 0 = 00000000	(11,0) R = 100 = 01100100 G = 100 = 01100100 B = 100 = 01100100	(11,0) R = 101 = 01100101 G = 100 = 01100100 B = 100 = 01100100
(0,12) R = 28 = 00011100 G = 97 = 01100001 B = 83 = 01010011	(12,0) R = 100 = 01100100 G = 100 = 01100100 B = 100 = 01100100	(12,0) R = 101 = 01100101 G = 100 = 01100100 B = 101 = 01100101

4. KESIMPULAN

1. Steganografi keamanan data (gambar) merupakan hal yang sangat penting didalam dunia modern saat ini. Hal ini semakin diperkuat dengan kebutuhan bisnis untuk menjaga kerahasiaan data yang sangat penting untuk dirahasiakan.
2. Algoritma Least Significant Bit dan End Of File untuk meningkatkan keamanan sebuah gambar. Gambar yang bersifat rahasia akan disisipkan kedalam gambar sehingga gambar tersebut tetap aman dari orang-orang yang bermaksud memanipulasi gambar tersebut.
- 3.

5. SARAN

Untuk pengembangan lebih lanjut, maka penulis memberikan saran-saran sebagai berikut :

1. Untuk penelitian selanjutnya diharapkan dapat dikembangkan menjadi sistem yang berbasis Web.
2. Penelitian dapat dikembangkan dengan menggunakan atau menambahkan algoritma yang lain, seperti algoritma RSA, Base64, Hill Cipher dan lain-lain.

DAFTAR PUSTAKA

- [1] Jumrin.; Sutardi, dan Subardin. 2016. Aplikasi Sistem Keamanan Basis Data Dengan Teknik Kriptografi *RC4 Stream Cipher*, *semanTIK*. Vol.2, No.1
- [2] Marisman,A.F, dan A.Hidayati. 2015. Pembangunan Aplikasi Pembanding Kriptografi Dengan *Caesar Cipher* dan *Advance Encryption Standart (AES)* Untuk File Teks,*Jurnal Penelitian Komunikasi dan Opini Publik*.Vol.19 No.3
- [3] Pabokory,F.N.; I.F.Astuti, dan A.H.Kridalaksana. 2015. Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen dan File Dokumen menggunakan Algoritma *Advanced Encryption Standard*, *Jurnal Informatika Mulawarman*.Vol.10 No.1.